BORDER BASES AND ORDER IDEALS: A POLYHEDRAL CHARACTERIZATION

GÁBOR BRAUN AND SEBASTIAN POKUTTA

ABSTRACT. Border bases arise as a canonical generalization of Gröbner bases. Unfortunately, so far only border bases containing a reduced Gröbner basis can be computed. In this note we extend our previous work [4] to arbitrary order ideals and devise a polyhedral characterization of order ideals and border bases: order ideals that support a border basis correspond one-to-one to integral points of the order ideal polytope. In particular, we establish a crucial connection between the ideal and its combinatorial structure. Based on this characterization we adapt the classical border basis algorithm to allow for computing border bases for arbitrary order ideals, which are *independent* of term orderings. We also show that finding a preference-optimal order ideal that supports a border basis is NP-hard.

1. INTRODUCTION

In this note we extend our previous work [4] to arbitrary order ideals. For the sake of completeness and self-containment we include the necessary preliminaries from [4] and establish the connection whenever appropriate. Gröbner bases have been essential in commutative algebra to make important operations on ideals such as intersection, membership test, elimination, projection, and many more *computationally accessible* allowing to perform actual computations with ideals. Recently it became clear though that Gröbner bases are not always the best choice in order to perform such operations. In particular when the actual ideals under consideration are inferred from measured data.

Although every Gröbner basis with respect to a degree-compatible term ordering can be extended to a border basis (see [12, p. 281ff]), not every border basis is an extension of a Gröbner basis and thus the former constitutes a broader class of bases. Even if an order ideal has the right cardinality, it does not necessarily support a border basis. Both cases were exemplified in [12, Example 6]. The border basis algorithm as formulated in [12], which in turn is a specification of Mourrain's generic algorithm [18], computes border bases of zero-dimensional ideals. Unfortunately, it does so for order ideals supported by a degree-compatible term ordering only and the computed border basis is supported by a reduced Gröbner basis. It therefore falls short to compute border bases for more general order ideals. In [12, Proposition 5], an alternative algorithm was presented which can *potentially* compute more general border bases *but requires a priori knowledge* of the order ideal that might support the border basis. Thus the algorithm allows for computing a border bases once the order ideal is known but does not solve the characterization problem itself. Further, the actual algorithm is heavily based on Gröbner basis computations which is unsatisfactory as pointed out in [12, p. 284].

In many cases though it can be advantageous to compute border bases for order ideals that do not necessarily stem from a degree-compatible term ordering. It has been an open question to characterize the admissible order ideals of a given zero-dimensional ideal. This question has been answered for degree-compatible order ideals in [4] (not to confuse with degree-compatible term orderings!). We will extend our previous results to provide a full characterization of all admissible order ideals. The concept of border bases and in particular the border basis algorithm is rather old and (re-)appeared in different fields of mathematics including computer algebra, discrete optimization, logic, and cryptography

independently under different names (see e.g.,[3, 17, 18])). A coherent framework was introduced in [11, 12, 13] and [16, Section 6.4].

In discrete mathematics and combinatorial optimization, Alon's *polynomial method* (cf. [1, 2]) and variants of the border basis algorithm have been used to formulate and test satisfiability of large classes of combinatorial problems (see e.g., [9, Section 2.3], [8, 7], and references contained therein). Another link between border bases and the Sherali–Adams closure, a method for convexification used in combinatorial optimization, was recently investigated in [20]. Border bases also have applications in cryptography where sparse quadratic systems have to be solved. These systems arise when rewriting the S-boxes of crypto systems as polynomial equations. For example, the celebrated XL, XSL, Mutant-tXL attacks (see e.g., [14, 5]) are essentially equivalent to the reformulation-linearization-technique of Sherali and Adams.

Our contribution. Due to its dependence on degree-compatible orderings, the classical computation of border bases can only provide border bases supported by a reduced Gröbner basis. These border bases do represent only a rather small fraction of all possible border bases (see [4, Example 2.6]) and border bases that have a particularly *nice* vector space basis often cannot be obtained by a degree-compatible term ordering. We will *free the computation of a border basis from the term ordering* by applying the theory of combinatorial optimization and polyhedral combinatorics to the combinatorial structure of zero-dimensional ideals. Our contribution is the following:

Polyhedral characterization of all border bases. We revisit the polyhedral characterization of border bases for degree-compatible order ideals introduced in [4] and extend it to arbitrary border bases. As a result, we provide a complete, polyhedral characterization of all border bases of any zero-dimensional ideal I. We associate an *order ideal polytope P* to I whose integral points are in one-to-one correspondence with order ideals supporting a border basis of I. This explicitly establishes the link between the combinatorial structure of the basis of the factor space and the structure of the ideal. Whether an order ideal supports a border basis is solely determined by the combinatorial structure of the order ideal polytope. A related result for Gröbner bases of the vanishing ideal of generic points was established in [19].

Computing arbitrary border bases. We extend the algorithm in [4] which in turn is based on the classical border basis algorithm (cf. [12]) and show how to compute border bases for arbitrary order ideals using the order ideal polytope without relying on a specific degree-compatible term ordering.

Computing optimal order ideals. We will show that computing an optimal order ideal supporting a border basis with respect to a linear preference function on the monomials is NP-hard in general. As we merely ask for a basis transformation this is surprising in some sense. Interestingly, the NP-hardness does not stem from the hardness of computing the L-stabilized span, as the problem remains NP-hard, even in cases where the L-stabilized span is small enough to be determined efficiently as shown in our reduction.

Computational feasibility. The computational feasibility of our method has been shown in [4] for degree-compatible order ideals and translates directly to the more general setting here (we have one rather large block rather than several small ones).

Outline. We start with the necessary preliminaries in Section 2. In Section 3 we introduce the order ideal polytope and establish a bijection between its integral points and border bases (for a given ideal I). In Section 4 we show how to compute border bases for generic order ideals. Finally, in Section 5 we establish the NP-hardness of computing optimal order ideals.

2. PRELIMINARIES

We consider a polynomial ring $K[\mathbb{X}]$ over the field K with indeterminates $\mathbb{X} = \{x_1, \ldots, x_n\}$. For convenience we define $x^m := \prod_{j \in [n]} x_j^{m_j}$ for $m \in \mathbb{N}^n$ and let $\mathbb{T}^n := \{x^m \mid m \in \mathbb{N}^n\}$ be the *monoid*

of terms. For any $d \in \mathbb{N}$ we let $\mathbb{T}^n_{\leq d} := \{x^m \in \mathbb{T}^n \mid \|m\|_1 \leq d\}$ be the set of monomials of total degree at most d. For a polynomial $p \in K[\mathbb{X}]$ with $p = \sum_{i=1}^{l} a_i x^{m_i}$ we define the *support of p* to be $\mathrm{supp}(p) := \{x^{m_i} \mid i \in [l]\}$ and similarly, for a set of polynomials $P \subseteq K[\mathbb{X}]$ we define the *support of P* to be $\mathrm{supp}(P) := \bigcup_{p \in P} \mathrm{supp}(p)$. Given a term ordering σ, the *leading term* $\mathrm{LT}_\sigma(p)$ of a polynomial p is $\mathrm{LT}_\sigma(p) := t$ with $t \in \mathrm{supp}(p)$ such that for all $t' \in \mathrm{supp}(P) \setminus \{t\}$ we have $t >_\sigma t'$; the *leading coefficient* $\mathrm{LC}_\sigma(p)$ of p is the coefficient of $\mathrm{LT}_\sigma(p)$. We drop the index σ if the ordering is clear from the context. Recall that the *degree of a polynomial* $p \in K[\mathbb{X}]$ is $\deg(p) := \max_{x^m \in \mathrm{supp}(p)} \|m\|_1$. The *leading form* $\mathrm{LF}(p)$ of a polynomial $p = \sum_{i=1}^{l} a_i x^{m_i} \in K[\mathbb{X}]$ is defined to be $\mathrm{LF}(p) = \sum_{i=1,\|m_i\|=d}^{l} a_i x^{m_i}$ where $d = \deg(p)$, i.e., we single out the part with maximum degree. Both LF and LT generalize to sets in the obvious way, i.e., for a set of polynomials P we define $\mathrm{LF}(P) := \{\mathrm{LF}(p) \mid p \in P\}$ and $\mathrm{LT}(P) := \{\mathrm{LT}(p) \mid p \in P\}$.

In the following we will frequently switch between considering polynomials $M = \{p_1, \ldots, p_s\}$, the generated ideal, and the generated vector space whose coordinates are indexed by the monomials in the support of M. We denote the ideal generated by M as $\langle M \rangle_{K[\mathbb{X}]}$ and the vector space generated by M as $\langle M \rangle_K$. For $n \in \mathbb{N}$ we define $[n] := \{1, \ldots, n\}$. All other notation is standard as to be found in [6, 15]; we have chosen the border basis specific notation to be similar to the one in [12] where the border basis algorithm was first introduced in its current form.

Central to our discussion will be the notion of an order ideal:

Definition 2.1. Let $\mathcal{O}$ be a finite subset of $\mathbb{T}^n$. If for all $t \in \mathcal{O}$ and $t' \in \mathbb{T}^n$ such that $t' \mid t$ we have $t' \in \mathcal{O}$, i.e., $\mathcal{O}$ is closed under factors, then we call $\mathcal{O}$ an *order ideal*. Furthermore, the *border $\partial \mathcal{O}$* of a non-empty order ideal $\mathcal{O}$ is the set of terms $\partial \mathcal{O} := \{x_j t \mid j \in [n], t \in \mathcal{O}\} \setminus \mathcal{O}$. As an exception, we set $\partial \emptyset := \{1\}$ for the empty order ideal.

Recall that an ideal $I \subseteq K[\mathbb{X}]$ is zero-dimensional, if and only if $K[\mathbb{X}]/I$ is finite dimensional. The $\mathcal{O}$-border basis of a zero-dimensional ideal I is a special set of polynomials:

Definition 2.2. Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal with border $\partial \mathcal{O} = \{b_1, \ldots, b_\nu\}$. Further let $\mathcal{G} = \{g_1, \ldots, g_\nu\} \subseteq K[\mathbb{X}]$ be a (finite) set of polynomials and let $I \subseteq K[\mathbb{X}]$ be a zero-dimensional ideal. Then the set $\mathcal{G}$ is an *$\mathcal{O}$-border basis* of I if:

  (1) the polynomials in $\mathcal{G}$ have the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ for $j \in [\nu]$ and $\alpha_{ij} \in K$;
  (2) $\langle \mathcal{G} \rangle_{K[\mathbb{X}]} = I$;
  (3) $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$ as vector spaces.

If there exists an $\mathcal{O}$-border basis of I then the order ideal $\mathcal{O}$ *supports a border basis of I*.

Note that the condition $\langle \mathcal{G} \rangle_{K[\mathbb{X}]} = I$ is a consequence of $\mathcal{G} \subseteq I$, the particular form of the elements in $\mathcal{G}$, and $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$. More precisely, $\langle \mathcal{G} \rangle_{K[\mathbb{X}]} + \langle \mathcal{O} \rangle_K$ is closed under multiplication by the x_i, and hence it is an ideal. As it contains 1, it must be the whole ring, and hence $\langle \mathcal{G} \rangle_{K[\mathbb{X}]} = I$ by the modular law. See [13, Proposition 4.4.2] for another proof.

In particular, an order ideal $\mathcal{O}$ supports an $\mathcal{O}$-border basis of I if and only if $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$. Moreover, for any given order ideal $\mathcal{O}$ and ideal I the $\mathcal{O}$-border basis of I is unique as b_j has a unique representation in $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$ for all $j \in [\nu]$. Furthermore, as $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$ it follows that $|\mathcal{O}| = \dim \langle \mathcal{O} \rangle_K$ is invariant for all choices of $\mathcal{O}$. The requirement for I being zero-dimensional is a consequence of this condition as well, as $\partial \mathcal{O}$ (and in consequence $\mathcal{O}$) as part of the output of our computation should be finite. Clearly, as a vector space, I has a degree filtration, i.e., $I = \bigcup_{i \in \mathbb{N}} I^{\leq i}$ where $I^{\leq i} := \{p \in I \mid \deg(p) \leq i\}$. For a set of monomials $\mathcal{O}$ we define $\mathcal{O}^{=i} := \{m \in \mathcal{O} \mid \deg(m) = i\}$ (and similarly for $\leq$ instead of $=$). Recall that an order ideal $\mathcal{O}$ is called *degree-compatible* (to I) if

$$\dim \left\langle \mathcal{O}^{=i} \right\rangle_K = \dim \left\langle \mathbb{T}^n_{=i} \right\rangle_K - \dim \frac{I^{\leq i}}{I^{\leq i-1}}$$

for all $i \in \mathbb{N}$. Note that not all order ideals supporting a border basis of a given zero-dimensional ideal I have to be degree-compatible (see e.g., [4] for an example). Moreover, not every order ideal stems from a term ordering as shown in the following example:

Example 2.3 (A general order ideal). The homogeneous ideal having a Gröbner basis in the degree lexicographic term ordering

$$x_2^2 + x_1 x_2 + x_1^2, x_1 x_2^2, x_2^4$$

has the associated order ideal

$$\{1, x_1, x_2, x_1 x_2, x_2^2, x_2^3\}.$$

Via a basis change, we obtain another order ideal

$$\{1, x_1, x_2, x_1^2, x_2^2, x_2^3\},$$

which cannot come from a term ordering. The reason is that every Gröbner basis of the ideal must contain a polynomial with degree-two leading term, which therefore must be a multiple of the first generator $x_2^2 + x_1 x_2 + x_1^2$ modulo higher-degree terms. The degree-two leading term cannot be $x_1 x_2$ because if e.g., $x_1 < x_2$ then the term x_2^2 is larger then $x_1 x_2$. So the leading term must be either x_1^2 or x_2^2, which excludes the order ideal.

In fact, it turns out that border bases with order ideals coming from a (degree-compatible) term ordering do cover only a small fraction of all possible border bases as exemplified in [4, Example 2.6].

2.1. **Computing stable spans.** Without proofs, we recall the underlying stable span computation of the classical border basis algorithm introduced in [12] as it will serve as a basis for our algorithm. The interested reader is referred to [13, 11] for a general introduction to border bases and to [12] in particular for an introduction of the border basis algorithm. The classical border basis algorithm calculates border bases of zero-dimensional ideals with respect to an order ideal $\mathcal{O}$ which is induced by a degree-compatible term ordering σ by successively generating a vector space approximation of the ideal. These approximations are generated via the following vector space *neighborhood extensions*:

Definition 2.4. (cf. [12, Definition 7.1 and paragraph preceding Proposition 13]) Let V be a vector space. We define the *neighborhood extension of V* to be

$$V^+ := V + V x_1 + \cdots + V x_n.$$

For a finite set W of polynomials, its *neighborhood extension* is

$$W^+ = W \cup W x_1 \cup \cdots \cup W x_n.$$

Note that for a given set of polynomials W such that $\langle W \rangle_K = V$ we have $\langle W^+ \rangle_K = \langle W \rangle_K^+ = V^+$ as multiplication with x_i is a K-vector space homomorphism. It thus suffices to perform the neighborhood extension on a set of generators W of V.

Let F be a finite set of polynomials and let $L \subseteq \mathbb{T}^n$ be an order ideal, then $F \cap \langle L \rangle_K = \{f \in F \mid \text{supp}(f) \subseteq L\}$, i.e., $F \cap \langle L \rangle_K$ contains only those polynomials that lie in the vector space generated by L. Clearly, for $L = \mathbb{T}_{\leq d}^n$ we have $\langle F \rangle_K \cap \langle L \rangle_K = \langle F \rangle_K^{\leq d}$. Using the neighborhood extension we can define:

Definition 2.5. (cf. [12, Definition 10]) Let L be an order ideal and let F be a finite set of polynomials such that $\text{supp}(F) \subseteq L$. The set F is *L-stabilized* if $\langle F^+ \rangle_K \cap \langle L \rangle_K = \langle F \rangle_K$. The *$L$-stable span F_L* of F is the smallest vector space G containing F satisfying $G^+ \cap \langle L \rangle_K = G$.

A straightforward construction of the L-stable span of F is to inductively define the following increasing sequence of vector spaces:

$$F_0 := \langle F \rangle_K \quad \text{and} \quad F_{k+1} := F_k^+ \cap \langle L \rangle_K \text{ for } k > 0.$$

The union $\bigcup_{k \geq 0} F_k$ is the *L-stable span F_L* of F.

The set L represents our *computational universe* and we will be in particular concerned with finite sets $L \subseteq \mathbb{T}^n$. Note that L-stability is a property of the vector space and does not depend on the basis:

Remark 2.6. The L-stable span of a finite set F depends only on the generated vector space $\langle F \rangle_K$, as $\langle F^+ \rangle_K = \langle F \rangle_K^+$.

In the following we will explain how the L-stable span can be computed explicitly for $L = \mathbb{T}^n_{\leq d}$. We will use a modified version of Gaussian elimination as a tool, which allows us to extend a given basis V with a set W as described in the following:

Lemma 2.7. [12, Lemma 12] *Let $V = \{v_1, \ldots, v_r\} \subseteq K[\mathbb{X}] \setminus \{0\}$ be a finite set of polynomials such that $\mathrm{LT}(v_i) \neq \mathrm{LT}(v_j)$ whenever $i, j \in [r]$ with $i \neq j$ and $\mathrm{LC}(v_i) = 1$ for all $i \in [r]$. Further let $G = \{g_1, \ldots, g_s\}$ be a finite set of polynomials. Then Algorithm 2.8 computes a finite set of polynomials $W \subseteq K[\mathbb{X}]$ with $\mathrm{LC}(w) = 1$ for all $w \in W$, $\mathrm{LT}(u_1) \neq \mathrm{LT}(u_2)$ for any distinct $u_1, u_2 \in V \cup W$, and $\langle V \cup W \rangle_K = \langle V \cup G \rangle_K$. (V, W may be empty.)*

Algorithm 2.8 (Gaussian Elimination for polynomials—GaussEl).

> **Input:** V, G as in Lemma 2.7.
> **Output:** $W \subseteq K[\mathbb{X}]$ as in Lemma 2.7.

(1) *Let $H := G$ and $\eta := 0$.*
(2) *If $H = \emptyset$ then return $W := \{v_{r+1}, \ldots, v_{r+\eta}\}$ and stop.*
(3) *Choose $f \in H$ and remove it from H. Let $i := 1$.*
(4) *If $f = 0$ or $i > r + \eta$ then go to step (7).*
(5) *If $\mathrm{LT}(f) = \mathrm{LT}(v_i)$ then replace f with $f - \mathrm{LC}(f) \cdot v_i$. Set $i := 1$ and go to step (4).*
(6) *Set $i := i + 1$. Go to step (4).*
(7) *If $f \neq 0$ then put $\eta := \eta + 1$ and let $v_{r+\eta} := f / \mathrm{LC}(f)$. Go to step (2).*

We can now compute the L-stable span using the Gaussian elimination algorithm 2.8:

Lemma 2.9. [12, Proposition 13] *Let $L = \mathbb{T}^n_{\leq d}$ and $F \subseteq K[\mathbb{X}]$ be a finite set of polynomials supported on L. Then Algorithm 2.10 computes a vector space basis V of F_L with pairwise different leading terms.*

Algorithm 2.10 (L-stable span computation—LStabSpan).

> **Input:** F, L as in Lemma 2.9.
> **Output:** V as in Lemma 2.9.

(1) $V := \mathrm{GaussEl}(\emptyset, F)$.
(2) $W' := \mathrm{GaussEl}(V, V^+ \setminus V)$.
(3) $W := \{w \in W' \mid \mathrm{supp}(w) \subseteq L\} = \{w \in W' \mid \deg(w) \leq d\}$.
(4) *If $|W| > 0$ set $V := V \cup W$ and go to step (2).*
(5) *Return V.*

The rationale for computing a stable span approximation is due to the following proposition that serves as a criterion for testing whether an order ideal $\mathcal{O}$ supports a border basis.

Proposition 2.11. [12, Proposition 16] *Let L be an order ideal. Further let $\tilde{I}$ be an L-stabilized generating vector subspace of a zero-dimensional ideal $I \subseteq K[\mathbb{X}]$, i.e., $\tilde{I}^+ \cap \langle L \rangle_K = \tilde{I}$ and $\langle \tilde{I} \rangle_{K[\mathbb{X}]} = I$. If $\mathcal{O}$ is an order ideal such that $\langle L \rangle_K = \tilde{I} \oplus \langle \mathcal{O} \rangle_K$ and $\partial \mathcal{O} \subseteq L$ then $\mathcal{O}$ supports a border basis of I.*

We obtain the following corollary:

Corollary 2.12. *Let $\tilde{I}$ be an $\mathbb{T}^n_{\leq d}$-stabilized vector space satisfying $\tilde{I} + \langle \mathbb{T}^n_{\leq d-1} \rangle_K = \langle \mathbb{T}^n_{\leq d} \rangle_K$. Then $\langle \tilde{I} \rangle_{K[\mathbb{X}]} \cap \langle \mathbb{T}^n_{\leq d} \rangle_K = \tilde{I}$.*

Proof. We apply Proposition 2.11 with the choice $L := \mathbb{T}^n_{\leq d}$, $I := \left\langle \tilde{I} \right\rangle_{K[\mathbb{X}]}$ and $\mathcal{O} := \mathbb{T}^n_{\leq d} \setminus \mathrm{LT}(\tilde{I})$ where the leading terms are with respect to any degree-compatible term ordering. Clearly, $\left\langle \mathbb{T}^n_{\leq d} \right\rangle_K = \tilde{I} \oplus \langle \mathcal{O} \rangle_K$. The condition $\tilde{I} + \left\langle \mathbb{T}^n_{\leq d-1} \right\rangle_K = \left\langle \mathbb{T}^n_{\leq d} \right\rangle_K$ ensures that $\mathcal{O}$ consists of monomials of degree less than d, so $\partial \mathcal{O} \subseteq \mathbb{T}^n_{\leq d}$. Hence the proposition applies, and we obtain $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$. Together with $\left\langle \mathbb{T}^n_{\leq d} \right\rangle_K = \tilde{I} \oplus \langle \mathcal{O} \rangle_K$ this gives $I \cap \left\langle \mathbb{T}^n_{\leq d} \right\rangle_K = \tilde{I}$. $\qquad\square$

For a worst-case bound on d, we will use the dimension of $K[\mathbb{X}]/I$. The necessary technical background is the following lemma.

Lemma 2.13. *Let I be a zero-dimensional ideal of $K[\mathbb{X}]$, and let $d := \dim K[\mathbb{X}]/I$. Then*

(1) $I^{\leq d} \big/ I^{\leq d-1} \cong \left\langle \mathbb{T}^n_{=d} \right\rangle_K$,

(2) $\left\langle \mathbb{T}^n_{\leq d-1} \right\rangle_K \big/ I^{\leq d-1} \cong K[\mathbb{X}]/I$.

Proof. Choose a degree-compatible term ordering. The associated order ideal (as every order ideal of size d) contains monomials of degree less than d. This proves $I + \left\langle \mathbb{T}^n_{\leq d-1} \right\rangle_K = K[\mathbb{X}]$, from which the statements easily follow via the modular law. $\qquad\square$

The border basis algorithm decomposes into two components. The first one is the calculation of the L-stable span for $L = \mathbb{T}^n_{\leq d}$ for sufficiently large d (this is the main 'work') and the second component is the extraction of a border basis via the final reduction algorithm. Effectively, after using *any* degree-compatible term ordering in order to compute the L-stable span one can choose a different ordering with respect to which the basis can be transformed. This approach is very much in spirit of the FGLM algorithm, Steinitz's exchange lemma, and related basis transformation procedures. In Remark 2.6 it is shown that L-stability does not depend on the basis and thus any sensible basis transformation that results in an admissible order ideal $\mathcal{O}$ is allowed. In the following we will characterize all admissible order ideals.

3. The order ideal polytope

We will now introduce the *order ideal polytope P* (a 0/1 polytope) that characterizes all admissible order ideals that support a border basis (for a given zero-dimensional ideal I) in an abstract fashion independent of particular vector space bases for the stable span approximation. Its role will be crucial for the later computation (Algorithm 4.3) of border bases for general order ideals. We will first focus on its properties and structure, then in Section 4, we will consider the computational aspect. We will show that the integral points of the order ideal polytope are in bijection with those order ideals that support a border basis of a given zero-dimensional ideal I (Theorem 3.2). In order to do so, we approach the problem from a polyhedral point of view to capture the intrinsic combinatorics of having to ensure that $K[\mathbb{X}] = I \oplus \langle \mathcal{O} \rangle_K$ as vector spaces on the one hand and $\mathcal{O}$ being an order ideal on the other hand. The role of the polyhedral description becomes prominent in Section 4 when the directness of the sum $I \oplus \langle \mathcal{O} \rangle_K$ is rephrased in the language of matrices and vector space bases.

Definition 3.1. Let I be a zero-dimensional ideal. Its *order ideal polytope $P(I)$* is given by the system of inequalities in Figure 3.1.

To obtain a finite dimensional polytope, we bound the degree of the monomials by $\dim K[\mathbb{X}]/I$. This bound is large enough to contain the worst case.

We are ready to relate the order ideal polytope with order ideals. From now on, let $\Lambda(I)$ denote the set of order ideals (that support a border basis) of a zero-dimensional ideal I. If $\mathcal{O} \in \Lambda(I)$ we call $\mathcal{O}$ *admissible* (for I).

$$z_{m_1} \geq z_{m_2} \quad \forall m_1, m_2 \in \mathbb{T}^n_{\leq d-1} : m_1 \mid m_2$$

$$\sum_{m \in \mathbb{T}^n_{\leq d-1}} z_m = d$$

$$\sum_{m \in U} z_m \leq \dim \langle U \cup I \rangle_K / I$$
$$\forall U \subseteq \mathbb{T}^n_{\leq d-1} : |U| = d$$

$$z_m \in [0,1] \quad \forall m \in \mathbb{T}^n_{\leq d-1}$$

FIGURE 3.1. Order ideal polytope $P(I)$ with $d := \dim K[\mathbb{X}]/I$

Theorem 3.2. *Let I be a zero-dimensional ideal. There is a bijection between the set $\Lambda(I)$ of its order ideals and the set of integral points of the order ideal polytope of I. The bijection is given by*

$$\xi : z \in P(I) \cap \mathbb{Z}^{\mathbb{T}^n} \mapsto \mathcal{O}(z) := \{m \in \mathbb{T}^n \mid z_m = 1\}.$$

Proof. In fact, we will see that the order ideal polytope is defined exactly to this end. Obviously, the order ideals consist of monomials of degree smaller than the dimension d of the factor $K[\mathbb{X}]/I$, so restricting to these monomials is permissive.

First, the integral solutions z of Condition 3.4 are exactly the 0/1 points, i.e., the characteristic vectors of sets of terms $\mathcal{O}(z) := \{m \in \mathbb{T}^n_{\leq d-1} \mid z_m = 1\}$.

Second, it is easy to see that Condition 4.1 means that $\mathcal{O}(z)$ is indeed an order ideal, as whenever $m_1 \mid m_2$ and $m_2 \in \mathcal{O}(z)$, i.e., $z_{m_2} = 1$, then it follows that $z_{m_1} = 1$, i.e., $m_1 \in \mathcal{O}(z)$ as well.

In the third step we will provide an algebraic characterization of Conditions 3.2 and 3.3. Clearly, Condition 3.2 can be rewritten to

$$|\mathcal{O}(z)| = d.$$

We will now show that Condition 3.3 is equivalent to

$$\langle \mathcal{O}(z) \rangle_K \cap I = \{0\},$$

i.e., the image of $\mathcal{O}(z)$ is linearly independent in the factor $K[\mathbb{X}]/I$. Thus Conditions 3.2 and 3.3 together are equivalent to $K[\mathbb{X}] = I \oplus \langle \mathcal{O}(z) \rangle_K$, finishing the proof.

To prove our claim on Condition 3.3, we rewrite it similarly as before,

$$|U \cap \mathcal{O}(z)| \leq \dim \langle U \cup I \rangle_K / I,$$

i.e., the size of $U \cap \mathcal{O}(z)$ is at most the dimension of the vector space generated by the image of U in the factor $K[\mathbb{X}]/I$. This is obviously *necessary* for the image of $\mathcal{O}(z)$ to be linearly independent in the factor. (Here the size of U does not matter.)

For *sufficiency* choose $U := \mathcal{O}(z)$. Then the dimension of the vector space generated by the image of $\mathcal{O}(z)$ is at least $|\mathcal{O}(z)|$, so the image of $\mathcal{O}(z)$ is independent. $\square$

4. COMPUTING GENERAL BORDER BASES

We will now turn to actually computing general border bases using Theorem 3.2. Clearly, we cannot expect to be able to compute a border basis for *any* order ideal, simply as not every order ideal supports such a basis. Having the order ideal polytope at hand something slightly more subtle can be done: We can choose the order ideal by optimizing a linear (preference) function $c \in \mathbb{Z}^{\mathbb{T}^n}$ over the order ideal polytope. In his way, we can *search* for an order ideal with preferred monomials in its support (see Subsection 4.3). An obvious application is to count the number of border bases that exist for a given ideal.

Before we can turn to the actual computation though, we will revisit the order ideal polytope and provide a reformulation that is suitable for actual computations (Subsection 4.1). We will then show in Subsection 4.2 how to obtain an $\mathcal{O}$-border basis for $\mathcal{O} \in \Lambda(I)$ where $I \subseteq K[\mathbb{X}]$ is a zero-dimensional ideal.

4.1. The order ideal polytope revisited.

Classically, the computation of the border basis is performed by Gaussian elimination applied to the matrices obtained within LStabSpan. The order ideal for which we then compute the border basis is solely determined by the pivoting rule when performing the elimination step (i.e., which basis we choose). Term orderings ensure that we obtain an order ideal for which a border basis exists (given the correct d). If we would now pivot arbitrarily, which effectively means permuting columns, it is not clear that, first, the resulting ideal is an order ideal and, second, that it does actually support a border basis. We face the combinatorial problem that when permuting a column such that it will end up being an element of $\mathcal{O}$ we also have to ensure that all its divisors will also end up in $\mathcal{O}$. On the other hand, due to the dimensionality constraint we must choose an exactly determined amount of elements that will end up in $\mathcal{O}$. This problem of *faithful pivoting* is captured by the order ideal polytope as we will see now.

Throughout this subsection let $M = \bigcup_{i \in \mathbb{N}} M_i \subseteq K[\mathbb{X}]$ be a finite set of polynomials with degree-filtration $\{M_i \mid i \in \mathbb{N}\}$ that generates a zero-dimensional ideal $\langle M \rangle_{K[\mathbb{X}]} \subseteq K[\mathbb{X}]$ such that all $p \in M_i$ have degree i. Furthermore, for each $i \in \mathbb{N}$ we have an enumeration $M_i = \{p_{ij} \mid j \in [k_i]\}$ with $k_i \in \mathbb{N}$. In the following we assume that L is of the form $L = \mathbb{T}^n_{\leq d}$ where $d := \dim K[\mathbb{X}]/\langle M \rangle_{K[\mathbb{X}]}$. For the sake of clarity, we assume that M is L-stabilized and has in particular a convenient form. One might think of M being the output of the LStabSpan procedure, which is then brought into the following reduced form:

Definition 4.1. Let M be a finite set of polynomials of degree at most ℓ for some $\ell \in \mathbb{N}$. Then M is in *canonical form* if the leading term of any element of M does not occur in the other elements. Here we can freely choose leading terms of the polynomials with the only constraint that they have to be maximal-degree terms.

We give a visual interpretation of the definition. The coefficient matrix $A \in K^{M \times \mathbb{T}^n_{\leq \ell}}$ of M is the matrix where the rows are the elements of M, the columns are all the monomials of degree at most ℓ, and the entries are the coefficients of the terms in the elements of M. We use the convention that for terms t_1, t_2 with $\deg(t_1) > \deg(t_2)$ we put column t_1 to the left of column t_2. Similarly, we put leading terms of a polynomial to the left of the other terms. Now M is in *canonical form* if the matrix A has the structure as depicted in Figure 4.1, i.e., it consists of degree blocks and each degree block is maximally interreduced.

The degree blocks correspond to the leading forms of the polynomials in M. Any finite set can be brought into canonical form by applying Gaussian elimination and column permutations of terms with same degree if necessary. In particular, the output of the LStabSpan procedure can be easily brought into this form, which is convenient to work with.

We are ready to provide a computational reformulation of the definition of the order ideal polytope.

Lemma 4.2. Let M be $\mathbb{T}^n_{\leq d}$-stabilized and in canonical form and $\langle M \rangle^{\leq d}_K / \langle M \rangle^{\leq d-1}_K \cong \langle \mathbb{T}^n_{=d} \rangle_K$. Let $L := \mathbb{T}^n_{\leq d-1}$ and assume $d = |L| - |M|$. Then the order ideal polytope $P(M, L) \subseteq [0, 1]^L$ of $\langle M \rangle_{K[\mathbb{X}]}$ is given by the system of inequalities in Figure 4.2.

Proof. Let $I := \langle M \rangle_{K[\mathbb{X}]}$. The only difference between the systems in Figure 3.1 and Figure 4.2 is that Condition 3.3 is replaced by Condition 4.3. So we will show their equivalence modulo the other conditions.

First, Corollary 2.12 provides $I^{\leq d} = \langle M \rangle^{\leq d}_{K[\mathbb{X}]} = \langle M \rangle_K$. Applying Lemma 2.13 (2) gives $\langle L \rangle_K / \langle M \rangle_K \cong K[\mathbb{X}]/I$ as vector spaces, and so $d = |L| - |M| = \dim K[\mathbb{X}]/I$. If $U' \subseteq L$, then via the modular law, we
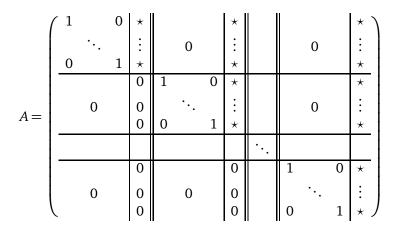
FIGURE 4.1. canonical form

(4.1)

(4.2)

(4.3)

$$\boxed{\begin{aligned} &z_{m_1} \geq z_{m_2} \quad \forall m_1, m_2 \in L : m_1 \mid m_2 \\ &\sum_{m \in L} z_m = d \\ &\sum_{m \in U} z_m \geq |U| - \mathrm{rk}(\tilde{U}) \\ &\qquad\qquad \forall U \subseteq L : |U| = |M| \\ &z_m \in [0,1] \quad \forall m \in L \end{aligned}}$$

FIGURE 4.2. Order ideal polytope $P(M, L)$. In Condition 4.3, the matrix $\tilde{U}$ is the induced sub-matrix of M with column monomials only in U.

have $\langle U' \cup I \rangle_K \big/ I \cong \langle U' \cup M \rangle_K \big/ \langle M \rangle_K$, so we can rewrite Condition 3.3 to

(4.4) $\displaystyle \sum_{m \in U} z_m \leq \dim \langle U' \cup M \rangle_K - |M|$

$$\forall U' \subseteq L : |U'| = \dim \langle L \rangle_K - |M|,$$

where we have deliberately replaced U with U'.

We will show that the difference of Conditions 4.2 and 4.3 is equal to Condition 4.4 with the choice $U' := L \setminus U$, which has size $|U'| = \dim \langle L \rangle_K - |M|$. This will finish the proof.

Let $U \subseteq L$ be as specified in Condition 4.3 and compute the difference of Conditions 4.2 and 4.3. We obtain

$$\sum_{m \in L \setminus U} z_m \leq \dim \langle L \rangle_K - |M| - |U| + \mathrm{rk}(\tilde{U}).$$

It is easy to see that $|U| = \dim \frac{\langle L \rangle_K}{\langle L \setminus U \rangle_K}$. We claim that it suffices to show that

$$\mathrm{rk}(\tilde{U}) = \dim \frac{\langle M \cup (L \setminus U) \rangle_K}{\langle L \setminus U \rangle_K}.$$

Indeed, using this we can rewrite the inequality as

$$\sum_{m \in L \setminus U} z_m \le \dim \langle L \rangle_K - |M| - \dim \frac{\langle L \rangle_K}{\langle L \setminus U \rangle_K}$$
$$+ \dim \frac{\langle M \cup (L \setminus U) \rangle_K}{\langle L \setminus U \rangle_K}$$
$$= \dim \langle M \cup (L \setminus U) \rangle_K - |M|,$$

which is (4.4) for $U' := L \setminus U$ as claimed.

We will show now that $\mathrm{rk}(\tilde{U}) = \dim \langle M \cup (L \setminus U) \rangle_K - \dim \langle L \setminus U \rangle_K$. Let B denote the matrix obtained when writing the elements in M as rows and let L index the columns. Clearly, $\langle L \rangle_K = \bigoplus_{\ell \in L} K e_\ell$ as a vector space and $\langle U' \rangle_K = \bigoplus_{\ell \in U'} K e_\ell$ as a sub vector space with $U' := L \setminus U$. We obtain $\langle L \rangle_K / \langle U' \rangle_K \cong \bigoplus_{\ell \in L \setminus U'} K e_\ell$. Note that $\langle M \rangle_K \subseteq \langle L \rangle_K$ and thus we can consider $\langle M \cup U' \rangle_K / \langle U' \rangle_K \subseteq \langle L \rangle_K / \langle U' \rangle_K$. Now $\dim \left(\langle M \cup U' \rangle_K / \langle U' \rangle_K \right) = \mathrm{rk}(\tilde{U})$ where $\tilde{U}$ is obtained from B by removing the columns in U'. We obtain

$$\mathrm{rk}(\tilde{U}) = \dim \frac{\langle M \cup U' \rangle_K}{\langle U' \rangle_K} = \dim \frac{\langle M \cup (L \setminus U) \rangle_K}{\langle L \setminus U \rangle_K}$$

and thus the result follows. □

4.2. **Computing border bases for $\mathcal{O} \in \Lambda(I)$.** As the computation of the L-stable span of a set of generators M is independent of the actual chosen vector space basis (see Remark 2.6), we can adapt the classical border basis algorithm (cf. [12]) to compute border bases for a general order ideal. We first determine the right computational universe $L = \mathbb{T}^n_{\le d}$ for some $d \in \mathbb{N}$ such that the associated L-stable span M contains all border bases. In a second step we optimize over the order ideal polytope $P(M, L)$ and then perform the corresponding basis transformation. We will first introduce the *generalized border basis algorithm*, and then establish its correctness:

Algorithm 4.3 (Generalized border basis algorithm—BBasis).

> **Input:** *F a finite generating set of a zero-dimensional ideal.*
> **Output:** *$\mathcal{G}$ a border basis of the ideal.*

(1) *Let $d := \max_{f \in F}\{\deg(f)\}$ and put $L := \mathbb{T}^n_{\le d}$.*
(2) *$M = \{m_1, \ldots, m_r\} := \mathtt{LStabSpan}(F, L)$.*
(3) *If $\mathbb{T}^n_{=d} \not\subseteq \mathrm{LT}(M)$ then set $d := d + 1$ and put $L := \mathbb{T}^n_{\le d}$ and go to step (2).*
(4) *Set $d_{old} := d$, $d := |L| - |M|$ and $L := \mathbb{T}^n_{\le d-1}$. If $d \le d_{old}$ then let $M := M^{\le d}$. Otherwise let $M := \mathtt{LStabSpan}(F, \mathbb{T}^{\le d})$.*
(5) *Choose $\mathcal{O} \in \Lambda(\langle M \rangle_{K[\mathbb{X}]})$ ($\Longleftrightarrow z \in P(M^{\le d-1}, L) \cap \mathbb{Z}^L$ and $\mathcal{O} = \mathcal{O}(z)$).*
(6) *Let $\mathcal{G} := \mathtt{BasisTransformation}(M, \mathcal{O})$.*

Note that step (3) is a convenient way to quickly check whether M is already L-stabilized and sufficiently large to calculate the dimension $K[\mathbb{X}]/I$. Step (4) adjusts d to this dimension and recomputes M.

In this augmented algorithm we added the steps (4), (5), and (6). Step (5) will be extensively discussed in Subsection 4.3 as there are various ways to determine $\mathcal{O} \in \Lambda(\langle M \rangle_{K[\mathbb{X}]})$ and this is precisely one of the main features, i.e., to choose the order ideal more freely. Note that by Theorem 3.2 we already know that $\mathcal{O}$ does support an $\mathcal{O}$-border basis of $\langle F \rangle_{K[\mathbb{X}]}$ (as $\langle F \rangle_{K[\mathbb{X}]} = \langle M \rangle_{K[\mathbb{X}]}$) and our task is now to actually extract this basis from M. This extraction is performed in step (6).

Let A be a matrix representing a set of polynomials where the columns correspond to the monomials in some fixed ordering. Let the *head* (short: $\mathtt{Head}(a)$) of a row a of A be the left-most monomial in the matrix representation whose coefficient is non-zero. Note that the notion of *head* replaces the notion

of *leading term* of a polynomial as we do not (necessarily) have a term ordering anymore. The main idea is to reorder the columns of M and then to bring M into a reduced row echelon form such that no $m \in \mathcal{O}$ is head of a row of the resulting matrix — a classical basis transformation:

Lemma 4.4. *Let $L = \mathbb{T}^n_{\leq \ell}$ with $\ell \in \mathbb{N}$, let M be a finite set of polynomials satisfying $\langle M \rangle_K = \langle M \rangle_{K[\mathbb{X}]} \cap \langle L \rangle_K$ and let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal with $\partial \mathcal{O} \subseteq L$ and $\mathcal{O} \in \Lambda(\langle M \rangle_{K[\mathbb{X}]})$. Then Algorithm 4.5 returns the $\mathcal{O}$-border basis $\mathcal{G}$ of $\langle M \rangle_{K[\mathbb{X}]}$.*

Proof. First, the algorithm finds ℓ from M. As $\mathcal{O} \in \Lambda(\langle M \rangle_{K[\mathbb{X}]})$ we have that $\mathcal{O}$ supports a border basis and in particular we have $K[\mathbb{X}] = \langle M \rangle_{K[\mathbb{X}]} \oplus \langle \mathcal{O} \rangle_K$, and hence $\langle L \rangle_K = \langle M \rangle_K \oplus \langle \mathcal{O} \rangle_K$ by the modular law. We will now show that Condition (1) of Definition 2.2 is satisfied. This in turn follows from the fact that the algorithm creates every element g_j of $\mathcal{G}$ to have the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ with $\alpha_{ij} \in K$. By construction $b_j \in \partial \mathcal{O}$ and thus $\mathcal{G}$ is an $\mathcal{O}$-border basis of $\langle M \rangle_{K[\mathbb{X}]}$. $\square$

Algorithm 4.5 (Basis transformation algorithm—`BasisTransformation`).

> **Input:** $M, \mathcal{O}$ as in Lemma 4.4.
> **Output:** $\mathcal{G}$ as in Lemma 4.4.

(1) *Set $\ell := \max_{m \in M} \deg(m)$.*
(2) *Permute the columns of M such that t is right of m in the matrix representation of M for all $m \in \mathbb{T}^n_{\leq \ell}$ and $t \in \mathcal{O}$.*
(3) *Reduce M using Gaussian elimination: like Algorithm 2.8, but use `Head` instead of LT and the coefficient of the head instead of LC. Let $\mathcal{G}'$ be the result.*
(4) *Let $\mathcal{G} := \{g \in \mathcal{G}' : \mathrm{Head}(g) \in \partial \mathcal{O}\}$.*
(5) *Return $\mathcal{G}$.*

We will show now that Algorithm 4.3 computes an $\mathcal{O}$-border basis for $\mathcal{O} \in \Lambda(I)$.

Proposition 4.6. *Let $F = \{f_1, \ldots, f_s\} \subseteq K[\mathbb{X}]$ be a finite set of polynomials that generates a zero-dimensional ideal $I = \langle F \rangle_{K[\mathbb{X}]}$. Then Algorithm 4.3 computes the $\mathcal{O}$-border basis $\mathcal{G}$ of I for any (chosen) $\mathcal{O} \in \Lambda(I)$.*

Proof. Corollary 2.12 ensures that upon reaching step (4), we have $\langle M \rangle_K = I^{\leq d}$. Via the modular law, step (4) sets d to the dimension $K[\mathbb{X}]/I$. The new M and d will also satisfy $\langle M \rangle_K = I^{\leq d}$. Obviously, $\mathbb{T}^n_{\leq d}$ contains all order ideals supporting a border basis, i.e., all $\mathcal{O} \in \Lambda(I)$ and even the boundary of these order ideals. Observe that $I = \langle F \rangle_{K[\mathbb{X}]} = \langle M \rangle_{K[\mathbb{X}]}$ and thus, by Lemma 4.4, it follows that $\mathcal{G}$ is indeed an $\mathcal{O}$-border basis of $\langle F \rangle_{K[\mathbb{X}]}$. $\square$

4.3. **Computing preferred border bases.**

Let M and L be as obtained after step (4) in Algorithm 4.3. As shown in Theorem 3.2 and Lemma 4.2, the order ideal polytope $P(M^{\leq d-1}, L)$ characterizes all admissible order ideals of $\langle M \rangle_{K[\mathbb{X}]}$. In particular, this shows that we cannot expect that every order ideal $\mathcal{O}$ supports an $\mathcal{O}$-border basis of $\langle M \rangle_{K[\mathbb{X}]}$ as the characterization is one-to-one. The natural question is therefore how to *specify* which order ideal should be computed, i.e., which $z \in P(M^{\leq d-1}, L) \cap \mathbb{Z}^L$ to choose. As the coordinates of z are in direct correspondence with the monomials in L we can define:

Definition 4.7. A *preference* is a vector $c \in \mathbb{Z}^L$ which assigns a weight to each monomial $m \in L$. If $z \in P(M^{\leq d-1}, L) \cap \mathbb{Z}^L$, then cz is the *score* or *weight* of z.

As $P(M^{\leq d-1}, L) \subseteq [0, 1]^n$ is a polytope we can compute an order ideal that has maximal score, i.e., we can compute $z_0 \in P(M^{\leq d-1}, L) \cap \mathbb{Z}^L$ such that

$$cz_0 = \max\{cz \mid z \in P(M^{\leq d-1}, L) \cap \mathbb{Z}^L\},$$

with associated order ideal $\mathcal{O}(z_0)$. In this sense a preference is an indirect way of specifying an order ideal. For certain choices of $c \in \mathbb{Z}^L$ though it can be hard to compute the order ideal that maximizes the score as we will show now.

5. Complexity of order ideals

In this section, we show that finding a weight optimal, admissible order ideal of a zero-dimensional ideal given by generators is NP-hard (Theorem 5.2). The hardness result is unexpected in the sense that we merely ask for a *nice* basis transformation. On the other hand it highlights the crucial role of order ideals in describing the combinatorial structure of the ideal.

From a practical point of view this is not too problematic as, although NP-hard, computing a weight optimal order ideal is no harder than actually computing the LStabSpan in general. Further, state-of-the-art mixed integer programming solvers that can solve the optimization problem such as scip, cplex, or gurobi can handle instance sizes far beyond the point for which the actual border bases can be computed (see [4]).

We will show the NP-hardness of finding an order ideal that supports a border basis with maximum score by a reduction from the k-Clique problem. The latter is well known to be NP-complete (see, e.g., [10]). Given a graph $\Gamma = (V, E)$, recall that a *clique C* is a subset of V such that for all distinct $u, v \in C$ we have $(u, v) \in E$.

k-Clique: Let $\Gamma = (V, E)$ be a graph. Determine whether Γ contains a clique C of size k.

We consider the following problem:

Max-Order ideal: Let $M \subseteq K[\mathbb{X}]$ be a system of polynomials generating a zero-dimensional ideal and let $c \in \mathbb{Z}^{\mathbb{T}^n}$ be a preference on the monomials. Compute an order ideal $\mathcal{O}_0$ supporting an $\mathcal{O}_0$-border basis of $\langle M \rangle_{K[\mathbb{X}]}$ with maximum score with respect to c, i.e.,

$$c(\xi^{-1}(\mathcal{O}_0)) = \max\{c(\xi^{-1}(\mathcal{O})) \mid \mathcal{O} \text{ admissible for } \langle M \rangle_{K[\mathbb{X}]}\}.$$

We will show that for every graph $\Gamma = (V, E)$ and $k \in [|V|]$ there exists a system of polynomials $F_{|V|,k} \subseteq K[x_v \mid v \in V]$ spanning a zero-dimensional ideal such that solving the Max-Order ideal problem for $F_{|V|,k}$ solves the k-Clique problem for Γ. For this, we construct an ideal encoding all k-cliques of the complete graph on n vertices: Let $n \in \mathbb{N}$ and $k \in [n]$ and define

$$F_{n,k} := \{v_j \mid j \in [n-k]\} \cup \mathbb{T}^n_{=3}$$

with $v_j := \sum_{i \in [n]} i^j x_i$. We consider the ideal generated by $F_{n,k}$. We show that its order ideals are in one-to-one correspondence with the k-element subsets of the set of n variables $x_1, \dots, x_n$ as stated in the following lemma.

Lemma 5.1. *Let $n \in \mathbb{N}$ and $k \in [n]$. Then $F_{n,k}$ generates a zero-dimensional ideal such that $\mathcal{O} \in \Lambda\left(\left\langle F_{n,k} \right\rangle_{K[\mathbb{X}]}\right)$ if and only if $\mathcal{O}^{=1} \subseteq \mathbb{T}^n_{=1}$ with $|\mathcal{O}^{=1}| = k$, $\mathcal{O}^{=2} = \{xy \mid x, y \in \mathcal{O}^{=1}\}$, and $\mathcal{O}^{=\ell} = \emptyset$ for all $\ell \geq 3$.*

Proof. We start by providing an explicit representation of the factor ring $K[x_1, \dots, x_n] \big/ \left\langle F_{n,k} \right\rangle_{K[\mathbb{X}]}$. The polynomials v_j with $j \in [n-k]$ are homogeneous of degree one. The coefficient matrix $A := (v_j)_{j \in [n-k]}$ is actually a Vandermonde matrix and in particular every square submatrix of A is invertible. In particular, removing the columns belonging to any k variables of $\{x_1, \dots, x_n\}$ from A, without loss of generality say, $x_1, \dots, x_k$, the resulting square submatrix is invertible. Thus, $\{x_1, \dots, x_k, v_1, \dots, v_{n-k}\}$ is a basis for the homogeneous polynomials of degree one, and hence the ring is also a polynomial ring in these variables. In particular,

$$\langle \mathcal{O} \rangle_K \cong K[x_1, \dots, x_n] \big/ \left\langle F_{n,k} \right\rangle_{K[\mathbb{X}]} \cong K[x_1, \dots, x_k] \big/ \left\langle \mathbb{T}^k_{=3} \right\rangle_{K[\mathbb{X}]}.$$

As substitution preserves degrees, homogeneity, etc., it follows, that any order ideal has to have $|\mathcal{O}^{=1}| = k$, $\mathcal{O}^{=2} = \{xy \mid x, y \in \mathcal{O}^{=1}\}$, and $\mathcal{O}^{=\ell} = \emptyset$ for all $\ell \geq 3$.

The other direction follows immediately as each order ideal $\mathcal{O}$ with $|\mathcal{O}^{=1}| = k$, $\mathcal{O}^{=2} = \{xy \mid x, y \in \mathcal{O}^{=1}\}$, and $\mathcal{O}^{=\ell} = \emptyset$ for all $\ell \geq 3$ is actually an order ideal such that $K[x_1, \ldots, x_n] = \left\langle F_{n,k} \right\rangle_{K[\mathbb{X}]} \oplus \langle \mathcal{O} \rangle_K$, as above. $\qquad\square$

Note that the order ideals of $F_{n,k}$ indeed correspond to the k-cliques of the complete graph on n vertices: If $\mathcal{O} \in \Lambda(F_{n,k})$, then $\mathcal{O}^{=1} = \{x_{i_1}, \ldots, x_{i_k}\}$ and $x_{i_j} x_{i_l} \in \mathcal{O}^{=2}$ if and only if $x_{i_j}, x_{i_l} \in \mathcal{O}^{=1}$. If we now remove all elements of the form $x_{i_j}^2$ with $x_{i_j} \in \mathcal{O}^{=1}$, and there are k of those, then

$$|\mathcal{O}^{=2} \setminus \{x_{i_j}^2 \mid x_{i_j} \in \mathcal{O}^{=1}\}| = \frac{k(k-1)}{2},$$

the size of a k-clique. It is worthwhile to observe that all admissible order ideals supporting a border basis of $\left\langle F_{n,k} \right\rangle_{K[\mathbb{X}]}$ are degree-compatible as $F_{n,k}$ is a homogeneous system. Thus the reduction presented in [4] would also establish NP-hardness in the general case. We will now present a more direct reduction not relying on the degree-compatible case.

Theorem 5.2. MAX-ORDER IDEAL *is NP-hard.*

Proof. The proof is by a reduction from the NP-hard k-CLIQUE. Let the graph $\Gamma = (V, E)$ with $n := |V|$ and $k \in [n]$ be an instance of k-CLIQUE. We consider $M := F_{n,k}$ and define $c \in \mathbb{Z}^{\mathbb{T}_{\leq 3}^n}$ via

$$c_m = \begin{cases} 1, & \text{if } m = x_u x_v \text{ and either } (u, v) \in E \text{ or } u = v; \\ 0, & \text{otherwise.} \end{cases}$$

By Lemma 5.1, the order ideals of $\langle M \rangle_{K[\mathbb{X}]}$ are in one-to-one correspondence with the k-cliques of the complete graph on n vertices. A vertex $v \in V$ is represented by the degree-one monomial x_v and each edge $(u, v) \in E$ is represented by the degree-two monomial $x_u x_v$. Thus, the score of an order ideal is the sum of k and the number of edges in Γ between the k vertices of the clique.

Clearly, there exists an admissible order ideal $\mathcal{O}$ with score $\frac{k(k+1)}{2}$ if and only if Γ contains a clique of size k. We obtain that MAX-ORDER IDEAL solves k-CLIQUE and so the former has to be NP-hard. $\qquad\square$

REFERENCES

[1] N. Alon. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, 8:7–29, 1999.
[2] N. Alon, M.B. Nathanson, and I.Z. Ruzsa. The polynomial method and restricted sums of congruence classes. *Journal of Number Theory*, 56:404–417, 1996.
[3] W. Auzinger and H.J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Proceedings of the International Conference on Numerical Mathematics*, pages 11–30. National University of Singapore, May 31-June 4, 1988, Birkhäuser, 1988.
[4] G. Braun and S. Pokutta. A polyhedral approach to border bases. *submitted / arxiv:0911.0859*, 2009.
[5] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. *Lecture Notes in Computer Science*, 1807:392–407, 2000.
[6] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2007.
[7] J.A. De Loera, J. Lee, P.N. Malkin, and S. Margulies. Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation - ISSAC '08*, 2008.
[8] J.A. De Loera, J. Lee, S. Margulies, and S. Onn. Expressing Combinatorial Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz. *Combinatorics, Probability and Computing*, 18(4):551–582, 2009.
[9] J.A. De Loera, P.N. Malkin, and P.A. Parrilo. Computation with polynomial equations and inequalities arising in combinatorial optimization. *preprint*, 2009.
[10] M.R. Garey, D.S. Johnson, et al. *Computers and Intractability: A Guide to the Theory of NP-completeness*. wh freeman San Francisco, 1979.
[11] A. Kehrein and M. Kreuzer. Characterizations of border bases. *Journal of Pure and Applied Algebra*, 196:251–270, 2005.
[12] A. Kehrein and M. Kreuzer. Computing border bases. *Journal of Pure and Applied Algebra*, 205:279–295, 2006.

[13] A. Kehrein, M. Kreuzer, and L. Robbiano. An algebraist's view on border bases. In *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, pages 169–202. Springer, 2005.

[14] M. Kreuzer. Algebraic attacks galore! *Preprint*, 2009.

[15] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1*. Springer, 2000.

[16] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Springer, 2005.

[17] H.M. Möller. Systems of algebraic equations solved by means of endomorphisms. *Lecture Notes in Computer Science*, 673:43–56, 1993.

[18] B. Mourrain. A new criterion for normal form algorithms. *Lecture Notes in Computer Science*, 1719:430–443, 1999.

[19] S. Onn and B. Sturmfels. Cutting corners. *Advances in Applied Mathematics*, 23(1):29–48, 1999.

[20] S. Pokutta and A.S. Schulz. On the connection of the Sherali-Adams closure and border bases. submitted, 2009. Available from: `http://www.optimization-online.org/DB_HTML/2009/08/2378.html`.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, REÁLTANODA U 13–15, 1053, HUNGARY
E-mail address: `braung@renyi.hu`

FACHBEREICH MATHEMATIK, TECHNISCHE UNIVERSITÄT DARMSTADT, GERMANY
E-mail address: `pokutta@mathematik.tu-darmstadt.de`